

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-173254

(43)Date of publication of application : 20.06.2003

(51)Int.Cl.

G06F 7/58

G09C 1/00

H03K 3/84

(21)Application number : 2002-183967

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 25.06.2002

(72)Inventor : FUJITA SHINOBU

UCHIDA KEN

KOGA JUNJI

OBA RYUJI

(30)Priority

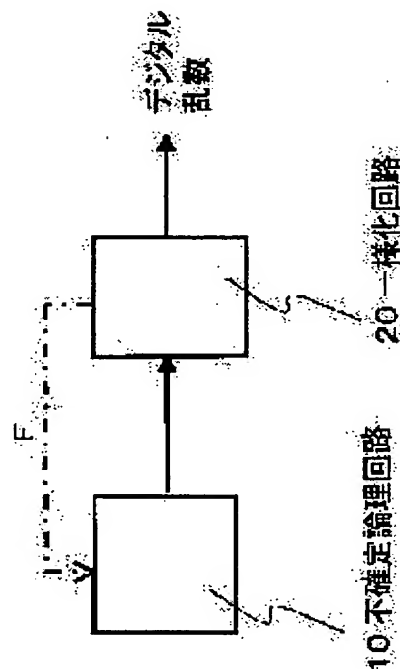
Priority number : 2001294836 Priority date : 26.09.2001 Priority country : JP

(54) RANDOM NUMBER FORMING CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a random number forming circuit generating random numbers having a high trueness degree, and transformable into a small integrated circuit.

SOLUTION: This random number forming circuit is provided with an indefinite logical circuit including a flip-flop type logical circuit for imparting a digital output value univocally undetermined to a digital input value, and a uniformizing circuit including an exclusive logical sum arithmetic circuit for equalizing an appearance frequency of '0' and '1' in the digital output value outputted from the indefinite logical circuit.



LEGAL STATUS

[Date of request for examination]

30.09.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3604674

[Date of registration] 08.10.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-173254

(P2003-173254A)

(43) 公開日 平成15年6月20日 (2003.6.20)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 7/58		G 0 6 F 7/58	A 5 J 0 4 9
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 B 5 J 1 0 4
H 0 3 K 3/84		H 0 3 K 3/84	Z

審査請求 未請求 請求項の数 8 O L (全 15 頁)

(21) 出願番号 特願2002-183967 (P2002-183967)

(22) 出願日 平成14年6月25日 (2002.6.25)

(31) 優先権主張番号 特願2001-294836 (P2001-294836)

(32) 優先日 平成13年9月26日 (2001.9.26)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 藤田 忍

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(72) 発明者 内田 建

神奈川県横浜市磯子区新杉田町8番地 株

式会社東芝横浜事業所内

(74) 代理人 100088487

弁理士 松山 允之 (外1名)

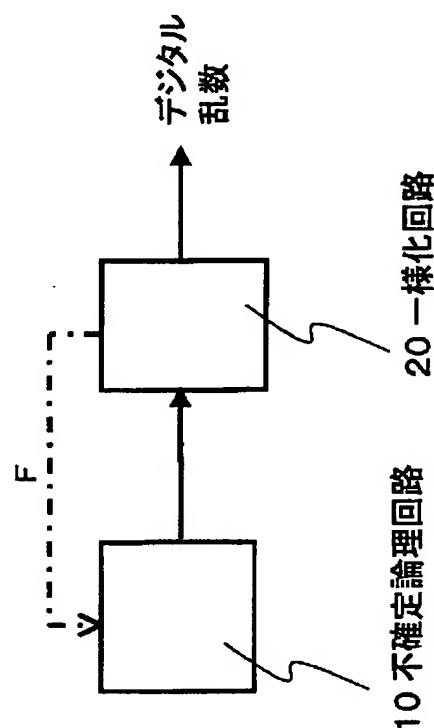
最終頁に続く

(54) 【発明の名称】 乱数生成回路

(57) 【要約】

【課題】 真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することを目的とする。

【解決手段】 デジタル入力値に対して一義的に決定されないデジタル出力値を与えるフリップフロップ型の論理回路を含む不確定論理回路と、前記不確定論理回路から出力される前記デジタル出力値における「0」と「1」の出現頻度を均等にするための排他的論理和演算回路などを含む一様化回路と、を備えた乱数生成回路を提供する。



【特許請求の範囲】

【請求項1】 デジタル入力値に対して一義的に決定されないデジタル出力値を与えるフリップフロップ型の論理回路を含む不確定論理回路と、前記不確定論理回路から出力される前記デジタル出力値における「0」と「1」の出現頻度を均等にするための一様化回路と、を備えたことを特徴とする乱数生成回路。

【請求項2】 前記不確定論理回路は、前記フリップフロップ型の論理回路の出力を前の状態を保持した出力とするための入力信号を継続的に与えつつ、前記フリップフロップ型の論理回路の前の状態に関する情報が実質的に消去される時間あるいはそれ以上の時間に亘って前記フリップフロップ型の論理回路に対する電源をオフするフェイズと、前記フリップフロップ型の論理回路に対する電源をオンするフェイズとを交互に繰り返すことにより、前記フリップフロップ型の論理回路から不確定なデジタル信号列を出力させることを特徴とする請求項1記載の乱数生成回路。

【請求項3】 前記フリップフロップ型の論理回路は、RS型のフリップフロップであり、前記不確定論理回路は、前記RS型のフリップフロップに対する入力S及び入力Rとして、前の状態を保持した出力を得るための入力データの組み合わせと、フリップフロップとして無効となる入力データの組み合わせと、を交互に入力することにより前記RS型のフリップフロップからの出力を連続的に不確定とすることを特徴とする請求項2記載の乱数生成回路。

【請求項4】 前記一様化回路は、前記フリップフロップ型の論理回路から出力される「0」と「1」の出現頻度をカウントするカウント回路と、前記カウント回路によりカウントした前記出現頻度に基づいたフィードバック信号を前記フリップフロップ型の論理回路に与えるフィードバック回路と、を有することを特徴とする請求項1～3のいずれか1つに記載の乱数生成回路。

【請求項5】 前記一様化回路は、前記不確定論理回路から出力された複数のデジタル信号の排他的論理和を演算し、乱数として出力することを特徴とする請求項1～4のいずれか1つに記載の乱数生成回路。

【請求項6】 前記一様化回路は、「0」と「1」との出現頻度が1:1であるデジタル信号列と、前記不確定論理回路から出力されるデジタル信号列と、の排他的論理和を演算し、デジタル乱数列として出力することを特徴とする請求項1～4のいずれか1つに記載の乱数生成回路。

【請求項7】 前記不確定論理回路は、4つ以上の偶数のNOR回路またはNAND回路を含み、これらNOR回路またはNAND回路は、それぞれの回路の出力端子が

その次の回路の入力端子の一方に連鎖的に接続されてなるものであることを特徴とする請求項1記載の乱数生成回路。

【請求項8】 前記不確定論理回路は、複数のRS型のフリップフロップを含み、これらフリップフロップ毎に大きさが異なるパルス電圧を入力し、これらフリップフロップからの出力の排他的論理和を出力とするものであることを特徴とする請求項1記載の乱数生成回路。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、乱数生成回路に関し、特に、デジタル論理回路によりコンパクトに構成することが可能でしかも真性度が高い乱数を発生し、暗号アルゴリズムに用いても好適な乱数生成回路に関する。

【0002】

【従来の技術】 デジタル乱数は、確率過程を伴う現象のシミュレーションや、セキュリティに用いる暗号アルゴリズムでの暗号鍵の生成などに用いられる。従来、デジタル乱数としては、CPUで計算によって作られる「擬似乱数」が用いられてきた。この擬似乱数は、典型的には、「フィードバックシフトレジスタ」と呼ばれる論理回路で作られる。

【0003】 これに対して、抵抗やダイオードに発生する雑音を使って乱数を作り出す方式も実用化されている。この場合、乱数に偏りや周期性などは見られなくなり、「真性乱数」に近いものが得られる。このタイプの乱数生成回路においては、雑音源の素子に一定電流を流して発生する雑音をハイパスフィルター回路に通して、AC成分を取り出し、それをアナログ回路で増幅したのち、AD変換してデジタル化する。このとき、ある値を閾値として、それを越えるものを「1」、それ以下のものを「0」というようにする。さらに、出てきた乱数列は偏りが出るため、それをデジタル回路で補正してから用いる場合が多い。

【0004】

【発明が解決しようとする課題】 CPUで作る擬似乱数は、初めに与えた数字（種）が同じであれば、同じ乱数を発生させてしまうことや、レジスタの個数に基づく周期性をもってしまうため、乱数としては適当でないことが知られている。特に、セキュリティに用いる場合には、「暗号鍵」を破られる危険性を産む原因となる。

【0005】 一方、雑音を増幅するタイプだと、一般的に抵抗やダイオードの熱雑音やショット雑音はアナログ信号であり、また出力が小さいために、アナログ増幅回路の構成が大規模となり、集積化、小型化が困難である。特に、暗号セキュリティ機能を搭載したICカード等の小型機器に組み込むことは困難である。

【0006】 つまり、周期性を持たない質の高い乱数を発生させ、かつ小型の集積回路が必要とされつつある。

【0007】 小型化のためには、TTLやCMOS等の

デジタル回路で構成することが望ましい。しかし、デジタル回路は、基本的にある入力に対して同一の出力を与えるので、アルゴリズム的な処理で乱数を作ることしかできない。このため、フィードバックシフトレジスタと同様に疑似乱数しか作り出せない。

【0008】この矛盾を解決するためには、デジタル回路で、出力が不確定になる回路を作る必要がある。

【0009】本発明は、かかる課題の認識に基づいてなされたものである。すなわち、その目的は、真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することにある。

【課題を解決するための手段】上記目的を達成するため、本発明の乱数生成回路は、デジタル入力値に対して一義的に決定されないデジタル出力値を与える不確定論理回路と、前記不確定論理回路から出力される前記デジタル出力値における「0」と「1」の出現頻度を均等にするための一様化回路と、を備えたことを特徴とする。

【0010】上記構成によれば、真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することができる。

【0011】ここで、前記不確定論理回路は、フリップフロップ型の論理回路を含むものとすれば、デジタル回路で、出力が不確定になる回路として活用することができる。

【0012】また、前記不確定論理回路は、前記フリップフロップ型の論理回路の出力を前の状態を保持した出力とするための入力信号を継続的に与えつつ、前記フリップフロップ型の論理回路の前の状態に関する情報が実質的に消去される時間あるいはそれ以上の時間に亘って前記フリップフロップ型の論理回路に対する電源をオフするフェイズと、前記フリップフロップ型の論理回路に対する電源をオンするフェイズとを交互に繰り返すことにより、前記フリップフロップ型の論理回路から不確定なデジタル信号列を出力させるものとすれば、デジタル回路で出力が不確定になる回路を実現できる。

【0013】また、前記フリップフロップ型の論理回路は、RS型のフリップフロップであり、前記不確定論理回路は、前記RS型のフリップフロップに対する入力S及び入力Rとして、前の状態を保持した出力を得るための入力データの組み合わせと、フリップフロップとして無効となる入力データの組み合わせ、つまりフリップフロップの2つの出力が同じ値をとるような入力の組み合わせと、を交互に入力することにより前記RS型のフリップフロップからの出力を連続的に不確定とすれば、デジタル回路で、出力が不確定になる回路として用いることができる。

【0014】また、前記一様化回路は、前記フリップフロップ型の論理回路から出力される「0」と「1」の出現頻度をカウントするカウント回路と、前記カウント回路によりカウントした前記出現頻度に基づいたフィード

バック信号を前記フリップフロップ型の論理回路に与えるフィードバック回路と、を有するものとすれば、フリップフロップ型の論理回路からのデジタル出力列における「偏り」を抑制することができる。

【0015】また、前記一様化回路は、前記不確定論理回路からの出力された複数のデジタル信号の排他的論理和を演算し、乱数として出力するものとすれば、「偏り」のない乱数が得られる。

【0016】また、前記一様化回路は、「0」と「1」との出現頻度が1:1であるデジタル信号列と、前記不確定論理回路から出力されるデジタル信号列と、の排他的論理和を演算し、デジタル乱数列として出力するものとすれば、「偏り」のない乱数列が得られる。

【0017】また、前記不確定論理回路は、4つ以上のNOR回路またはNAND回路を含み、これらNOR回路またはNAND回路は、それぞれの回路の出力端子がその次の回路の入力端子の一方に連鎖的に接続されてなるものとすれば、ウェーハ上での素子特性の「ばらつき」などによる乱数の品質の低下を防ぎ、良質の乱数を生成する乱数生成回路を安定して量産することが容易となる。

【0018】なおここで、「連鎖的に接続」とは、例えば、4つのNOR回路を用いる場合には、第1のNOR回路の出力が第2のNOR回路の入力の一方に接続され、第2のNOR回路の出力が第3のNOR回路の入力の一方に接続され、第3のNOR回路の出力が第4のNOR回路の入力の一方に接続され、第4のNOR回路の出力が第1のNOR回路の入力の一方に接続されたような接続関係をいう。

【0019】また、前記不確定論理回路は、複数のRS型のフリップフロップを含み、これらフリップフロップ毎に大きさが異なるパルス電圧を入力し、これらフリップフロップからの出力の排他的論理和を出力とするものとすれば、「1」と「0」の出現確率の差を確実且つ容易に小さくすることができる。つまり、「1」と「0」の出力の偏りを減らして乱数の品質を高くすることができる。

【0020】

【発明の実施の形態】以下、図面を参照しつつ、本発明の実施の形態について詳細に説明する。

【0021】図1は、本発明の乱数生成回路の要部構成を表すブロック図である。

【0022】すなわち、本発明の乱数生成回路は、不確定論理回路10と、その出力を受ける一様化回路20とを備える。

【0023】不確定論理回路10は、デジタル回路で構成した論理回路であり、その論理回路の原理的にみて、特定の入力信号の組み合わせに対して出力の「0」または「1」が不確定になるものである。論理出力が不確定の場合、論理回路10を構成する素子のその時々物理

的な要因によって、出力が変動する。この物理現象を利用することにより、一定の入力に対して、出力が変動するデジタル回路が得られ、「0」と「1」とのランダムなデジタル信号列が得られる。

【0024】この方法で得られた「0」と「1」とのデジタル信号列の配列は、そのデジタル回路を構成する素子の特性に依存しているため、「0」と「1」の出現頻度に「偏り」が生ずる。

【0025】そこで、一様化回路20において、それらを再度デジタル処理して、偏りを無くして真性度の高いデジタル乱数を得る。または、同図にフィードバックループFとして表したように、一様化回路20は、不確定論理回路10の出力データに基づいたフィードバック信号を与え、出力データにおける「偏り」を抑制するようにしてもよい。

【0026】このようにすれば、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。

「0」と「1」の頻度を補正する回路も、比較的小規模な論理回路で構成可能である。

【0027】そして、乱数の元になる現象は、不確定論理回路10を構成する素子の物理現象に基づくものであるため、同一の入力に対して、不確定の出力が得られるため、乱数列に周期性が出ず、乱数を推定可能な疑似乱数とは異なる質の高い乱数を得ることができる。

【0028】以下、具体例を参照しつつ本発明の実施の形態についてさらに詳細に説明する。

【0029】(第1の実施例) 図2は、本実施例の乱数生成回路の基本構成を例示する模式図である。

【0030】すなわち、同図の乱数生成回路は、不確定論理回路10にRS型のフリップフロップ(RS-FF)10Aを設けている。

【0031】図3は、ここで用いるRS-FF10Aの具体的な構成を例示する模式図である。同図に表したように、RS-FF10Aは、2つのNOR論理回路11、12を組み合わせたものである。

【0032】ここで、入力 $S=R=0$ の場合、出力Qとしては、そのフリップフロップの前の出力Qと同じ値を出力する。しかし、電源が切れた状態が前の状態であると、再度電源を投入した後の出力は不確定となる。実際に $S=R=0$ を入力すると、NOR回路11、12を構成する複数のCMOSがON(オン)するタイミングの微妙な違いにより、「0」か「1」の出力が決まる。特性の微妙な差は常に一定ではなく、回路周囲の温度や、物理的に回路内に発生する微小な雑音などで決まるので、出力も一定でない。

【0033】図4は、このRS-FFの動作を表すパルス図である。

【0034】ここで、 $S=R=0$ としたまま、パルス的にNOR回路11、12の電源電圧 V_{cc} (V_{in})をON、OFFすることを、それぞれ「0」、「1」の入

力とする。フリップフロップの情報を完全に消去するのに十分な時間だけ「0」を入力した後、「1」を入力することによりフリップフロップの出力を不確定にすると、「1」の入力に対して、不確定な出力Qが得られる。従って、このように入力として「0」と「1」とを繰り返すと、図4に表したように出力Qとして、「0」または「1」の不確定でランダムな数値列が得られる。

【0035】但し、論理回路11、12を構成するトランジスタが完全には対称ではないため、「0」と「1」の出現頻度は均等でなく、どちらかに偏る。そこで、後述するように、「0」と「1」を均等にする回路20と組み合わせることにより、本発明の乱数生成回路が得られる。

【0036】なお、インバータを配列したデジタル回路を用いて乱数的なデジタル信号を生成させるものとしては、例えば、特開2001-166920号公報に開示されているように、デジタル回路に付加する素子の温度変動を用いるものがある。しかし、この従来技術の場合には、奇数個のインバータを環状接続したリングオシレータの発振周波数を温度に対して不安定にさせる点で、本願とは全く異なる。さらに、この従来技術の場合、全体構成が複雑で回路規模が大きいう点でも改善すべき点が多い。また、リングオシレータなどの正帰還型発振回路の場合、発振を開始するトリガーが、回路の基本クロックと同期したノイズ信号であるため、発振回路とクロックを完全に非同期にできないため、発生する乱数列に周期性が現れて、乱数の真性度が損なわれるという問題がある。

【0037】これに対して、本発明によれば、フリップフロップの不確定出力を積極的に作り出すことにより、はるかにコンパクトで効率的に乱数デジタル信号列を得ることができる。

【0038】さて、本発明においてRS型のフリップフロップを用いる場合、図5のように2つのNOR論理回路11、12を接続すると、上記具体例とは違った方式で不確定の出力を得ることができる。

【0039】図6は、その動作を説明するパルス図である。

【0040】この場合、電源 V_{cc} は通常どおりONにしておき、入力を $S=R$ として、図6に表したように、「1」と「0」を交互に入力する。 $S=R=0$ の場合は、出力Qは前の状態のQを保持し、出力/Q(「Qバー」を表す)は前の状態のQを保持して、それぞれ「0」か「1」の値をとる。

【0041】ところが、 $S=R=1$ の場合、 $Q=0$ と/ $Q=0$ で同じになってしまうので、その次に $S=R=0$ とするとQは1となるか、0となるか不確定となる。その結果として、図6に表したような不確定なデジタル信号列が得られる。

【0042】但し、この場合にも、得られるデジタル信

号列において、「0」と「1」との出現頻度は均等ではない場合が多いので、後述する「0」と「1」を均等にする回路20と組み合わせられることにより、本発明の乱数生成回路が得られる。

【0043】また、本発明の乱数生成回路における不確定論理回路10としては、図2乃至図6に表した具体例以外にも、これと同様に、D型フリップフロップの場合にはクロック入力を「0」に、JKフリップフロップの場合には $J=K=1$ または0に、またT型の場合には入力Tを任意の値にしておけば、フリップフロップの初期値が決まっていない場合に出力が不確定となり、上記と同様にして乱数生成回路を構成することができる。他の種類のフリップフロップも同様であり、要は、不確定な出力が利用できればよい。

【0044】(第2の実施例)次に、本発明の第2の実施例について説明する。

【0045】図7は、本実施例の乱数生成回路の不確定論理回路10の要部を表す模式図である。

【0046】すなわち、本実施例においては、不確定論理回路において、2つのCMOS回路13、14を並べ、ゲートとCMOSのトランジスタの間を相互に結線したフリップフロップ回路10Cを設ける。これは、MOSトランジスタT1がONすると、MOSトランジスタT3がOFFするフリップフロップである。

【0047】図8は、このフリップフロップ回路の動作を説明する模式図である。

【0048】電源を切っている状態では、全てのトランジスタはOFFであり、どの電極の電位もグランドと同じである。

【0049】そして、Vinを1(H:High)とすると、各トランジスタのゲートの電位は0(L:Low)であるので、トランジスタT1とトランジスタT3がON状態になりうるが、フリップフロップであるので、どちら一方のみがON状態となる。

【0050】仮に図8(a)に表したように、トランジスタT1が先にONしたとすると、トランジスタT1のソースとドレインは導通して等電位となり、A点の電位はVinと同じHighレベルになる。そうすると、トランジスタT3はOFFとなり、トランジスタT4がON状態となって安定化する。このときB点の電位、すなわち出力は初期のLow(0)のままである。

【0051】逆に、トランジスタT3が先にONしたとすると、図8(b)に表した状態となり、出力はHigh(1)となる。

【0052】このように、トランジスタT1とT3のどちらが早くONするかで、出力が決まる。どちらが速くONするかは不確定であり、前述した第1実施例と同様に出力が不確定なフリップフロップとなる。フリップフロップの電源のON、OFFを「0」、「1」のデジタル入力とすると、入力「1」に対して、「0」か「1」

が不確定の出力を出す。

【0053】ただし、2つのCMOSが完全に同一の特性を持っていないので、T1とT3のどちらが早くONするかには偏りが出る。これを、以下に詳述するように、一様化回路20により補正すれば、真性度の高いデジタル乱数を得ることができる。

【0054】(第3の実施例)次に、本発明の第3の実施例として、一様化回路20の具体例について詳細に説明する。

【0055】前述した第1及び第2実施例においては、不確定論理回路10の具体例としてフリップフロップ回路を用いた。しかし、前述したように、これらフリップフロップ回路から得られるデジタル信号列は、「0」と「1」の出現頻度が完全に均等ではなく、ある種の「偏り」を持っている。一様化回路20は、この「偏り」を補正するためのデジタル処理を行う。

【0056】図9は、本実施例における一様化回路の動作を説明するための概念図である。

【0057】同図に表したように、不確定論理回路10の出力を時系列的に、 Q_n, \dots, Q_{n+k} として、これらの $k+1$ 個のデータにXOR(排他的論理和)の論理演算を施す。その結果をTとする。不確定論理回路10の出力において、「1」の出現確率を p 、「0」の出現確率を $1-p$ とすると、Tが1となる確率は、 $0.5 + 0.5 \cdot (1 - 2p)^{k+1}$ となる。 k が大きくなるほど、確率が0.5に近づき、偏りが補正される。

【0058】前述した第1実施例において実際に試作したRS-FFでは、「偏り」が大きくほぼ $p=0.1$ であった。 $k=10$ の場合、Tが1となる確率は0.543となり、また $k=20$ の場合、0.505となり、また $k=30$ の場合、0.5005となって、0.5に近づき、ほとんど「偏り」がなくなる。

【0059】 k が大きくなると、乱数の生成速度が遅くなってしまうが、例えば電源をON、OFFする周期を30MHzにすると、 $k=30$ としても約1Mbit/秒の速度でデジタル乱数列を生成することができるので、実用上は問題とならない場合が多い。または、 Q_n, \dots, Q_{n+k} のXOR、 $Q_{n+1}, \dots, Q_{n+k+1}$ のXOR、 $Q_{n+2}, \dots, Q_{n+k+2}$ のXORというように、一つづつ、ずらして演算すれば、生成速度も損なわない。

【0060】また、このようにして得られた乱数列データをフィードバックシフトレジスタのシード(種)に使っても良い。

【0061】また、以下に説明するような方法を用いれば、簡便に「0」と「1」の出現確率を均等にすることができる。

【0062】すなわち、デジタル信号Pが「1」になる確率を p 、デジタル信号Qが「1」になる確率を q とすると、PとQとの排他的論理和(XOR)の演算値Tが

「1」となる確率と、「0」となる確率の差は、次式により表される。

$$4(0.5-p)(0.5-q) \cdots (1)$$

従って、「Pが「1」になる確率が0.5であれば、Qが「1」になる確率が0.5でなくても、PとQとの排他的論理和の演算値Tの「0」と「1」の出現確率は等しくなる。

【0063】ここで、図10に表したように、フリップフロップ10への入力信号を分岐してT型のフリップフロップ20Bに入れると、周期が2倍の信号になり、これはフリップフロップ10の出力と同じタイミングで「0」と「1」とが交互に並ぶ信号となる。この信号は、当然に「0」と「1」の出現率が等しい。従って、この信号とフリップフロップ10の信号との排他的論理和をとると、その演算出力Tにおいては当然に「0」と「1」の出現確率が等しく、真性度の高いデジタル乱数列として用いることができる。

【0064】また、図11に表したように、フィードバックシフトレジスタ(FSR)20Cにより、フリップフロップ10と同じクロックで作った擬似乱数Rは、「0」と「1」とを均等に出力するので、これとフリップフロップ10の出力との排他的論理和をとると、その演算値Tは「0」と「1」の出現率が等しく、真性度の高いデジタル乱数列として用いることができる。

【0065】また、2つのフリップフロップを利用した構成として、もうひとつの具体例を挙げることができる。

【0066】図12は、この具体例を表す模式図である。すなわち、T型フリップフロップで倍周期にしたものと、D型フリップフロップで均一化したものをXORする。

【0067】この場合には、2個の不確定フリップフロップ回路A及びBを使う。まず、基準クロック信号を2分割して、一方をT型フリップフロップに通して、周期が1/2になるようにして不確定フリップフロップAに入力する。すると、基準クロックの1/2周期の不確定ランダム信号Aが得られるが、「0」と「1」の出現率は、この段階では不均一である。

【0068】もう一方は、不確定フリップフロップBに通して、不確定出力QとQバーを得る。QバーをD型フリップフロップに通して、基準クロック一つ分遅らせてから、QとQバーを交互に出力すると、この信号は原理的に「0」と「1」とが50パーセントづつ配列するランダム信号Bとなる。但し、QとQバーが順番に並ぶので、この時点では規則性が現れる。こうして作ったランダム信号Aとランダム信号Bとの排他的論理和(XOR)をとると、先の2例と同様の原理で、0と1の出現率が均一な乱数が得られる。

【0069】(第4の実施例)次に、本発明の第4の実施例として不確定論理回路の出力をモニタしフィードバ

ックをかける乱数生成回路について説明する。

【0070】図13は、本実施例の乱数生成回路の要部構成を表す模式図である。

【0071】本実施例においては、第1及び第2の実施例として前述したような不確定フリップフロップの入力部に、一様化回路20がフィードバックを加える。このようなフィードバックにより、不確定フリップフロップの「0」と「1」の出現確率を均等に近くすることができる。

【0072】すなわち、同図において、A側にあるトランジスタT7が早くONすると、フリップフロップの出力が「0」になるとする。同図に表したように、フィードバック回路20Eと電源入力Vinとの間に同一の設計仕様を持つNチャンネルのMOSトランジスタT7、T8をそれぞれ設け、B側のトランジスタT8のゲートはグランドに落としておく。

【0073】フリップフロップの出力をデジタルカウンタ20Dでカウントしておき、「0」と「1」のカウントの差分に比例した電圧をA側のMOSトランジスタT7のゲートに与え、「1」の出力が多い場合に、A側のトランジスタT7のゲート電圧を少しプラスにシフトしてチャネル抵抗を相対的に低くして、A側に電流が流れやすくすると、A側が優先的に動作するので、出力「0」が増える。

【0074】逆に、「0」の出力が多い場合には、A側のトランジスタT7のゲート電圧をマイナスにして、チャネル抵抗を上げる。

【0075】こうしたフィードバックをかけることにより、フリップフロップの出力の「0」と「1」のずれを少なくすることができる。その結果、このまま乱数として使うことも出来る。

【0076】また、第3実施例として説明したように、「偏り」をなくす論理回路を組み合わせると、乱数の「偏り」をさらに小さくできる。この場合、前述したXORをとるデータkの数が少なく済むので、乱数の生成速度を上げることができる。

【0077】(第5の実施例)次に、本発明の第5の実施例として、不確定論理回路10において、フリップフロップを構成するNOR回路(またはNAND回路)の数を増やすことで、「0」と「1」の出力の偏りを減らす構成について説明する。

【0078】半導体回路を量産する場合、ウェーハ上での特性の「バラツキ」などにより、一部の出力に極端に偏りなどが生ずる場合がある。例えば、「0」の出現頻度が100パーセントにほぼ近くなるという回路が、全体の一部に出現する可能性がある。出力が極端に偏ると、平滑回路で補正しても乱数の質が高まらないため、乱数生成回路としては不良品となる。本実施例は、この不良品の出現を減らすために用いて好適なものである。

【0079】図14は、本実施例の構成を概念的に表す

模式図である。本実施例においては、偶数個のフリップフロップからの出力のXORをとる。すなわち、多数（偶数）のNOR回路（またはNAND回路）を図14の例示したように並べ、それぞれのNOR回路の出力がその次のNOR回路の入力の一方となるように連鎖的に接続した場合、不確定フリップフロップと同様の動作を行わせることができる。

【0080】つまり、入力（Input）が「1」の場合、各フリップフロップの出力は全て「0」となる状態が安定である。つまり、入力「1」は、リセット（R）信号であるといえる。続いて、入力を「0」にすると、NOR回路は、インバータと等価となるので、「1」と「0」が交互に出力される状態が安定である。つまり、入力「0」は、セット（S）信号であるといえる。そして、これらNOR回路からの出力が、順に「0」、「1」、「0」、「1」となるか、それとも、「1」、「0」、「1」、「0」となるかは、その前の状態を保持することにより決定されるが、その前の状態（入力として「1」を与えた状態）における出力が、「0」、「0」、「0」、「0」であるため、どちらになるか不確定となる。

【0081】この場合、多数のNOR回路が競合状態となるので、2つのNOR回路でフリップフロップを構成する場合よりも、出力の偏りが小さくなる。当然ながら、NOR回路の数が多いほど、出力の偏りも小さくなる。

【0082】この具体例の場合、奇数番目のNOR回路の出力どうしと、偶数番目のNOR回路の出力どうしは、原理的に同じ出力値となる。偶数番目または奇数番目の出力を前述した一様化回路と組み合わせることで、さらに良質の乱数を得ることができる。

【0083】次に、本実施例の第2の具体例として、偶数個のフリップフロップに発振回路からの信号を入力する構成について説明する。

【0084】図15は、本具体例の要部構成を例示する模式図である。すなわち、同図（a）に表したように、多数かつ偶数個のNOR回路（またはNAND回路）を並べて不確定フリップフロップを形成し、それぞれのNOR回路への入力を同図のように独立化させる。そして、それぞれに、「0」か「1」のいずれかと、「0」と、を交互に入力する。このようにすると、さらにランダム化の要素が増えるため、良質な乱数を作ることができる。

【0085】以下、この原理を図15のように4つのNOR回路からなる場合について説明する。各NOR回路への入力と出力の組合せを、便宜的に（X1、X2、X3、X4：Q1、Q2、Q3、Q4）と表すとすると、例えば、以下の如くとなる。

（1、0、0、0：0、1、0、1）
（1、1、0、0：0、0、1、0）

（1、0、1、0：0、1、0、1）
（1、0、0、1：0、1、0、0）
（1、1、1、0：0、0、0、1）

この時の出力Q1～Q4が、「0」と「1」とが交互に並ばない場合には、この次に、入力Xとして全て「0」を入力すると、NOR型回路は全てインバータと等価になるため、X及びQは、以下のいずれかとなる。

（0、0、0、0：0、1、0、1）
または（0、0、0、0：1、0、1、0）

この場合、そのどちらになるかは、不確定である。入力Xがランダム性を持っていると、不確定フリップフロップのランダム性との相乗効果により、乱数の質が向上する。ランダム入力のひとつの方法として、図16に例示したように、非同期で周波数の異なる発振回路を用いる方法が有効である。

【0086】すなわち、NOR回路のそれぞれに対応させて、非同期発振回路とD型ラッチを設ける。ここで、非同期発振回路は、その出力が「0」か「1」に変換されるように、出力端にバッファがついたものが望ましいが、マルチバイブレータのように出力がデジタル化されている場合には不用である。非同期発振回路からの出力は、標準クロックに合わせてラッチされ、そのラッチ信号とクロックのANDをとると、「0」か「1」のいずれかと、「0」と、が交互に並んだ信号が得られる。これらを入力Xとすれば、フリップフロップからの出力は、図15（b）に例示したように、確定値である「0」と、不確定値としての「0」か「1」のいずれか、を交互に出力する。不確定値を取り出すことで、デジタル乱数が得られる。

【0087】なおここで、X1からX4の独立入力を適当な確定出力を与える論理回路で処理しただけでは乱数は作ることはいできない。非同期であっても、各入力Xに周期性があるため、それらを論理回路で組み合わせただけでは、出力に必ず周期性が表れ、良質の乱数は一般に得られない。不確定フリップフロップを介して、始めて良質の乱数となる。

【0088】または、図17に例示したように、擬似乱数を発生するLFSR（Linear Feedback Shift Register）を使い、いずれかのシフトレジスタSRからランダム入力する方法も簡便で有効である。図17では、図16と違いNAND回路が2段で接続されているが、これは論理動作として、AND回路とNOR回路が2段で接続されている場合と、同様のものである。

【0089】原理的に、出力の奇数番目どうしと、偶数番目どうしは、同じ出力値となる。偶数番目または奇数番目の出力を前述した一様化回路20と組み合わせることで、さらに良質の乱数を得ることができる。

【0090】（第6の実施例）次に、本発明の第6の実施例として、前述した第5実施例とは別の方法により、不確定論理回路10において、フリップフロップを構成

するNOR回路（またはNAND回路）の数を増やして、「0」と「1」の出力の偏りを減らす構成について説明する。

【0091】図18は、本実施例の回路の要部を表す模式図である。同図(a)は、5つのUFFにより構成した具体例を表す。ここで、UFF(Unsetttable Flip-Flop)は、同図(b)に例示したように、NOR回路2個からなる不確定フリップフロップとすることができる。

【0092】UFFは、「0」と「1」の出力頻度が、入力パルス電圧の高さに依存する傾向がある。すなわち、入力パルスをデジタル回路の基準となる電源電圧VDDよりも小さくしていくと、UFFには、「1」の出力頻度が高くなっていくか、あるいは、低くなっていく傾向が見られる。これは、UFFを構成するそれぞれのNOR回路の閾値電圧に、小さいながらも「ばらつき」が存在するためである。

【0093】図19は、UFFに入力するパルス電圧に対する「1」の出現確率の依存性を例示するグラフ図である。すなわち、同図の具体例の場合、入力パルスの周期を2マイクロ秒、パルス幅を65ナノ秒とし、そのパルス電圧Vrsを変化させた時の、UFF出力の「1」の出現確率を表す。またこのUFFは、電源電圧VDDが2ボルトのものである。

【0094】図19から、パルス電圧Vrsが高くなるに従って、「1」の出現確率が連続的に増加していることが分かる。そして、パルス電圧Vrsがおよそ1.3ボルト弱の時に、「1」の出現確率がほぼ0.5となる。つまり、このパルス電圧を与えた場合、UFFの出力における「0」と「1」の出現確率はほぼ同一となる。

【0095】従って、図18に例示したように、複数個のUFFのそれぞれに異なった電圧のパルスを入力すると、いずれかのUFFにおいて、「0」と「1」の出力頻度の差が比較的小さい出力が得られる。

【0096】図18においては、5つのUFFに対する入力電圧を、VDDから、VDDの20パーセントまで順に減らしている。5つのUFFの出力の排他的論理和XORをとると、このXORの出力の「0」と「1」の出力頻度の差は、5つのUFFの中で「0」と「1」の出力頻度の差が一番小さいものと同程度か、それよりも小さくなる。この原理は、図9に例示した一様化回路20AのXORの作用として前述したものと同様である。図18は、5つのUFFを用いた場合を例示するが、UFFの数を増やして、それらの電源電圧を細かく変化させるほど、「0」と「1」の出力の偏りを減らす効果が高まる。

【0097】以上、具体例を例示しつつ本発明の実施の形態について説明した。しかし、本発明は、上述した各具体例に限定されるものではない。

【0098】例えば、本発明において用いる不確定論理回路および一様化回路の具体的な構成に関しては、上記の具体例に限定されず、その機能あるいは作用が同様な全ての回路に置換したのもも本発明の範囲に包含される。

【0099】例えば、出力が不確定なフリップフロップを複数個、並列もしくは直列に並べた論理回路の出力を、「0」と「1」とを均等にする論理回路に入力する形式の乱数生成回路も、同様に有効であり、本発明の範囲に包含される。

【0100】さらに、前述した複数の実施例のうち、不確定出力のデジタル回路と、デジタル出力の頻度を補正する回路とを部分的に組み合わせたものも、乱数生成回路として使用可能であり、本発明の範囲に包含される。

【0101】また、本発明の乱数生成回路によって作られたデジタル乱数は、そのまま使用することもできるが、フィードバックシフトレジスタの種として用いることにより、新たな乱数を生成することもできる。

【0102】

【発明の効果】以上詳述したように、本発明によれば、フリップフロップ型の論理回路などを利用することにより、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。

【0103】また同時に、「0」と「1」の頻度を補正する一様化回路も、比較的小規模な論理回路で構成可能である。

【0104】そして、乱数の元になる現象は、不確定論理回路を構成する素子の物理現象に基づくものであるので、同一の入力に対して、不確定の出力が得られるため、乱数列に周期性が出ず、乱数を推定可能な疑似乱数とは異なる質の高い乱数を得ることができる。

【0105】さらに、一定周期のクロック信号を分岐してT型のフリップフロップなどにより不確定論理回路の出力と同じタイミングで「0」と「1」とが交互に並ぶ信号を形成し、この信号と不確定論理回路の出力信号との排他的論理和をとると、その演算出力Tにおいては当然に「0」と「1」の出現確率が等しく、真性度の高いデジタル乱数列として用いることができる。

【0106】すなわち、本発明によれば、真性度の高い乱数をコンパクト且つ低価格で実現できるようになり、例えばICカードなどに応用してセキュリティーの確実な安価なカードシステムを実現できる点で産業上のメリットは多大である。

【図面の簡単な説明】

【図1】本発明の乱数生成回路の要部構成を表すブロック図である。

【図2】本発明の実施例の乱数生成回路の基本構成を例示する模式図である。

【図3】本発明の第1実施例において用いるRS-FF10Aの具体的な構成を例示する模式図である。

【図4】RS-FFの動作を表すパルス図である。

【図5】2つのNOR論理回路11、12を接続したRS-FFのもうひとつの具体例を表す模式図である。

【図6】図5のRS-FFの動作を説明するパルス図である。

【図7】本発明の実施例の乱数生成回路の不確定論理回路10の要部を表す模式図である。

【図8】本発明の実施例のフリップフロップ回路の動作を説明する模式図である。

【図9】本発明の実施例における一様化回路の動作を説明するための概念図である。

【図10】一様化回路のもうひとつの具体例を表す模式図である。

【図11】一様化回路のもうひとつの具体例を表す模式図である。

【図12】2つのフリップフロップを利用したもうひとつの具体例を表す模式図である。

【図13】本発明の実施例の乱数生成回路の要部構成を表す模式図である。

【図14】本発明の第5実施例の構成を概念的に表す模式図である。

【図15】本発明の第5実施例の具体例の要部構成を例

示する模式図である。

【図16】ランダム入力のひとつの方法として、非同期で周波数の異なる発振回路を用いた構成を表す模式図である。

【図17】擬似乱数を発生するLFSR (Linear Feedback Shift Resistor) を使い、いずれかのシフトレジスタSRからランダム入力する構成を表す模式図である。

【図18】本発明の第6実施例の回路の要部を表す模式図である。

【図19】UFFに入力するパルス電圧に対する「1」の出現確率の依存性を例示するグラフ図である。

【符号の説明】

10 不確定論理回路

10A~10C フリップフロップ型の論理回路

11、12 NOR型論理回路

13、14 MOSトランジスタ

20 一様化回路

20A XOR回路

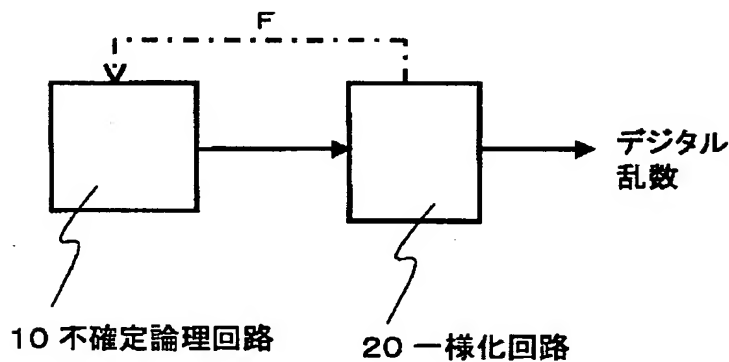
20B T型フリップフロップ

20C FSR

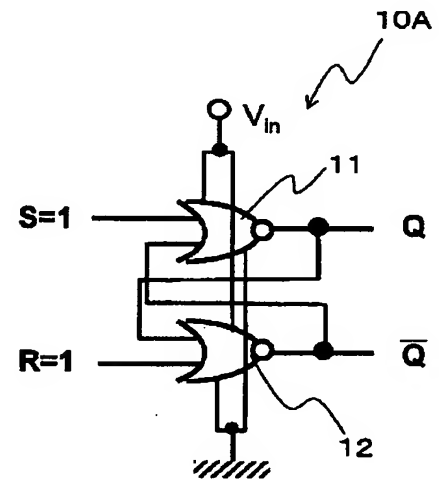
20D デジタルカウンタ

20E フィードバック回路

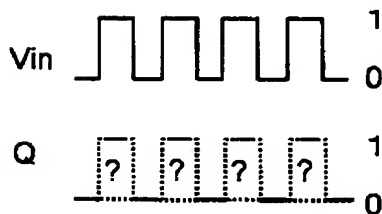
【図1】



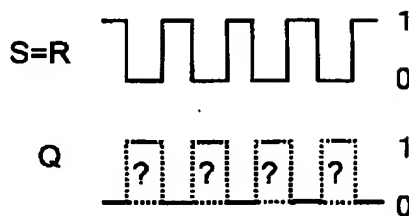
【図3】



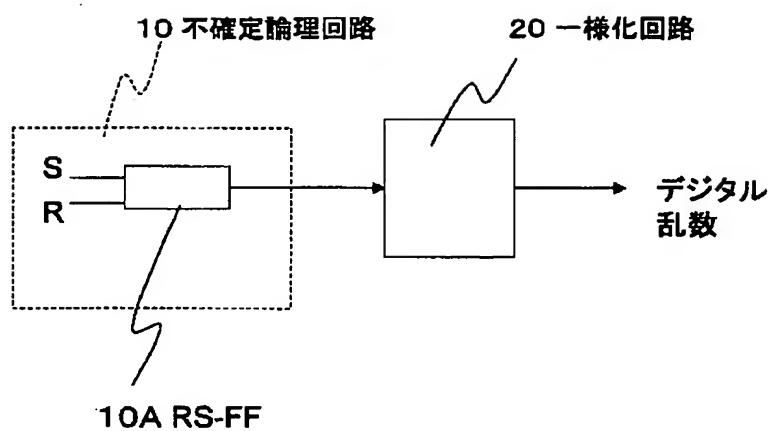
【図4】



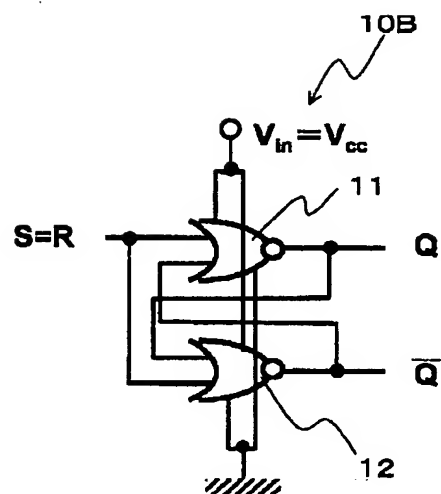
【図6】



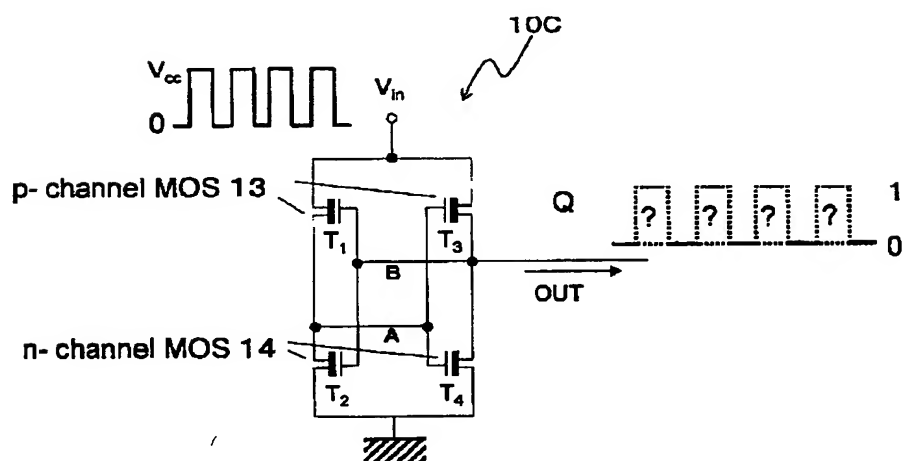
【図2】



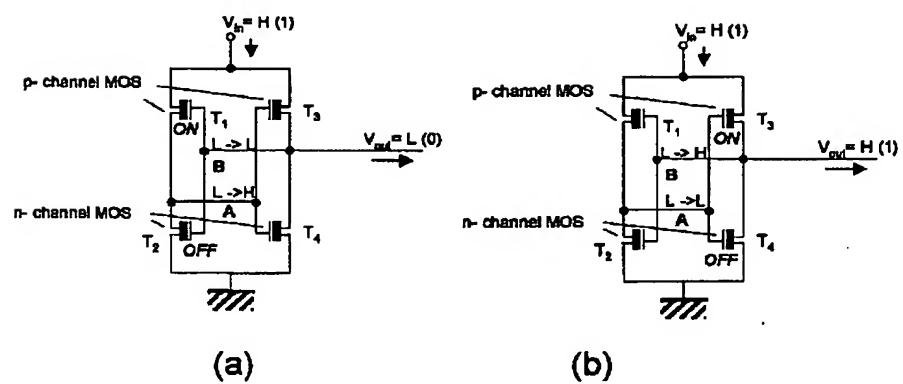
【図5】



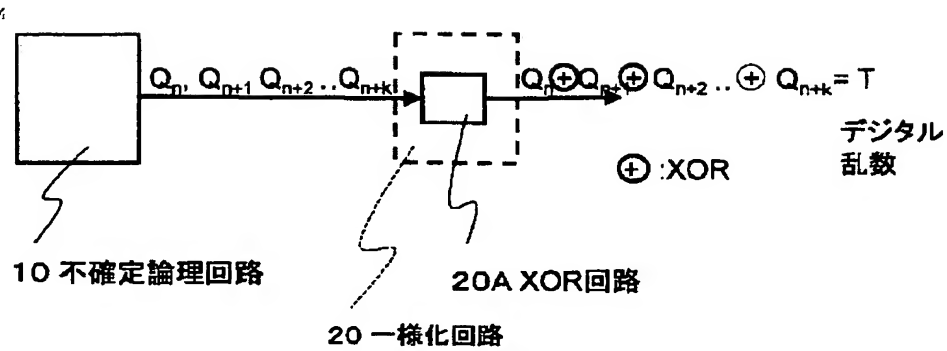
【図7】



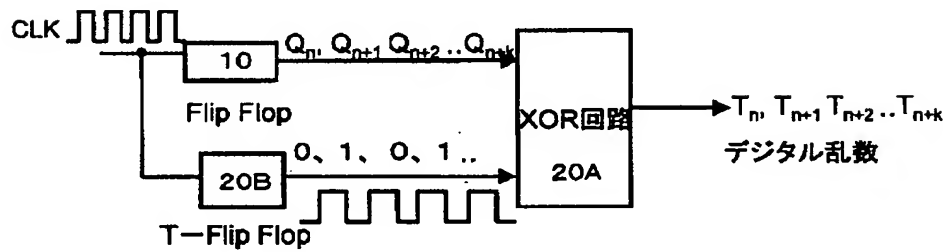
【図8】



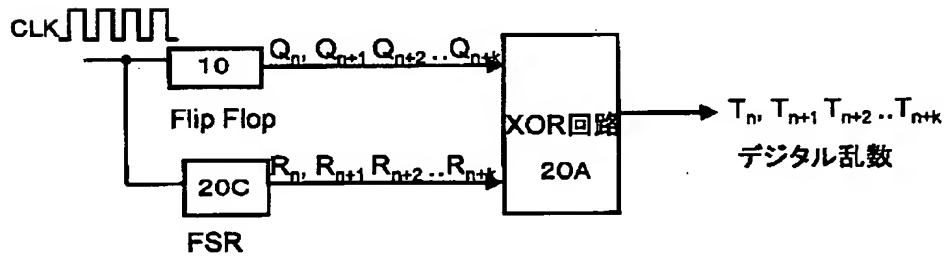
【図9】



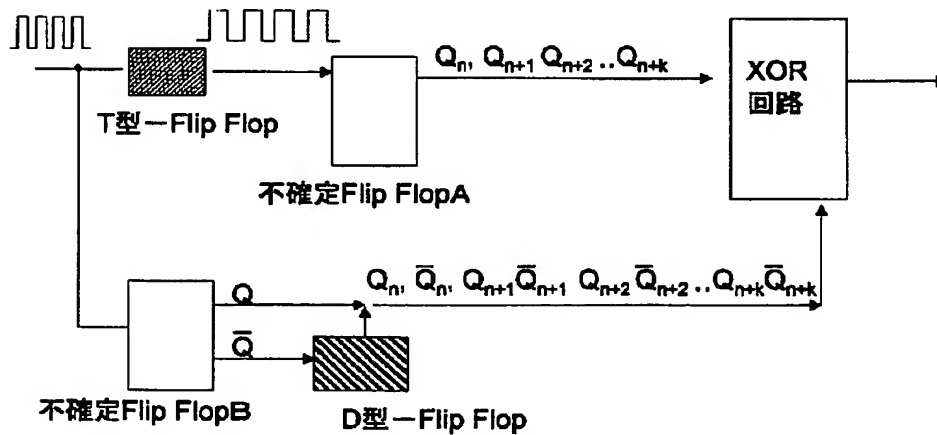
【図10】



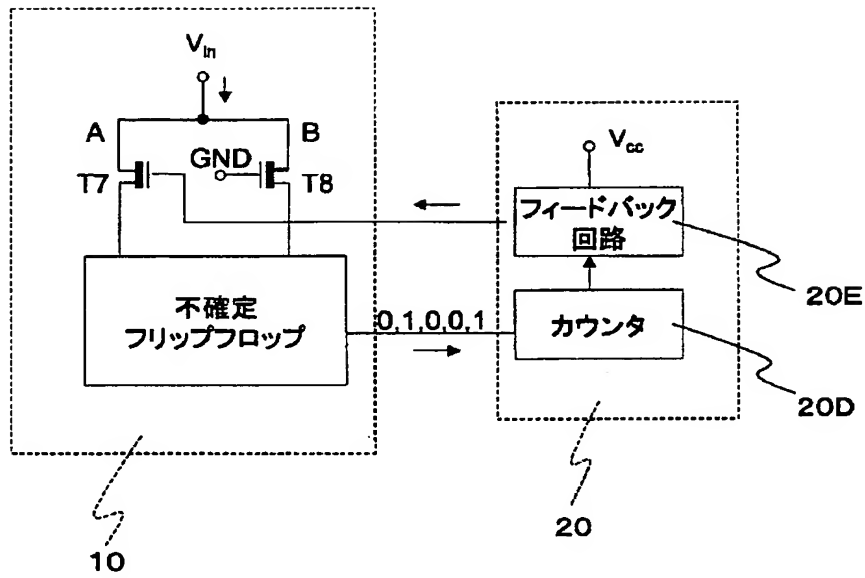
【図11】



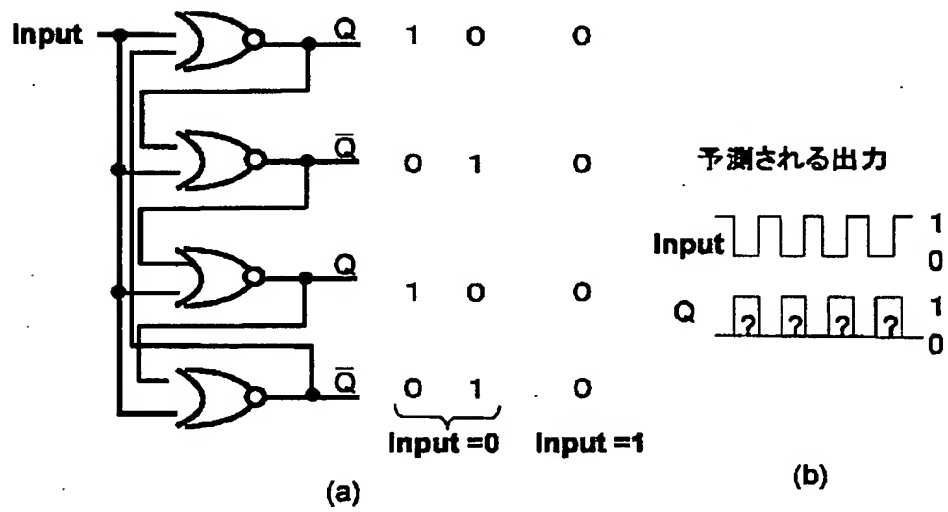
【図12】



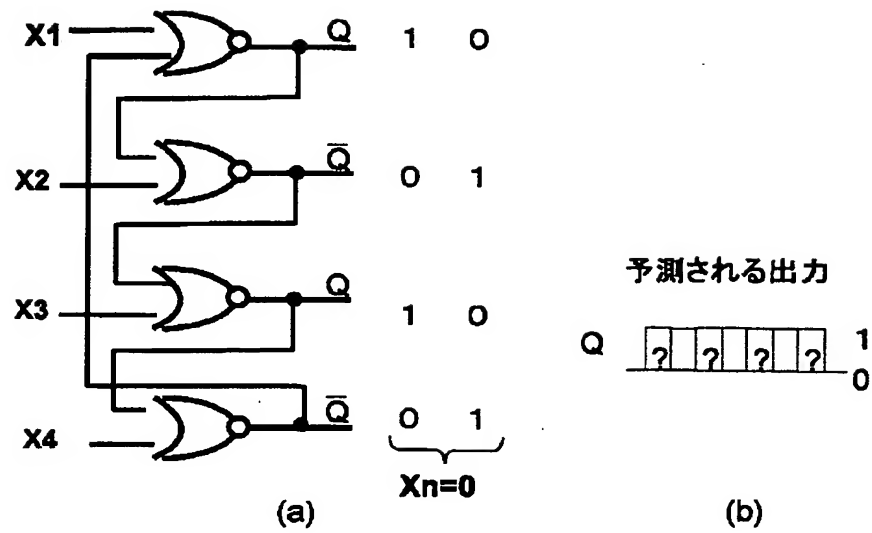
【図13】



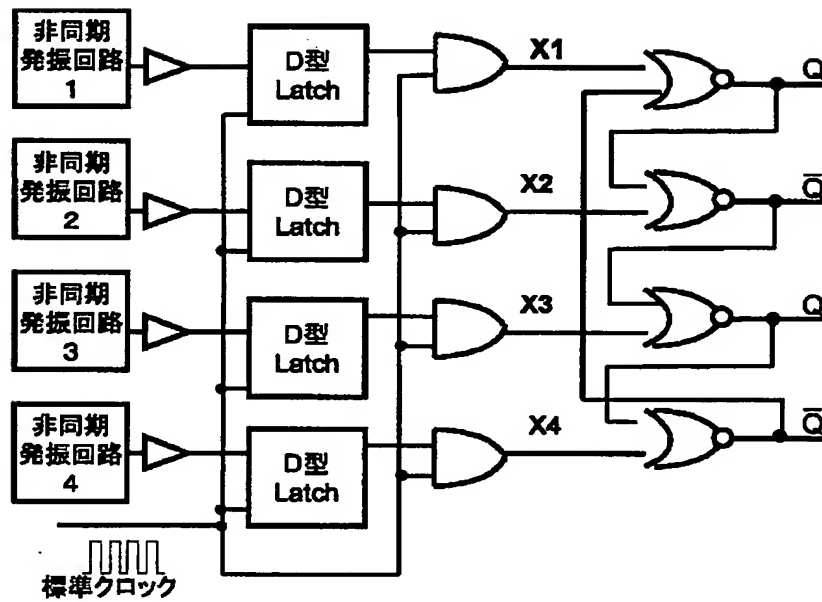
【図14】



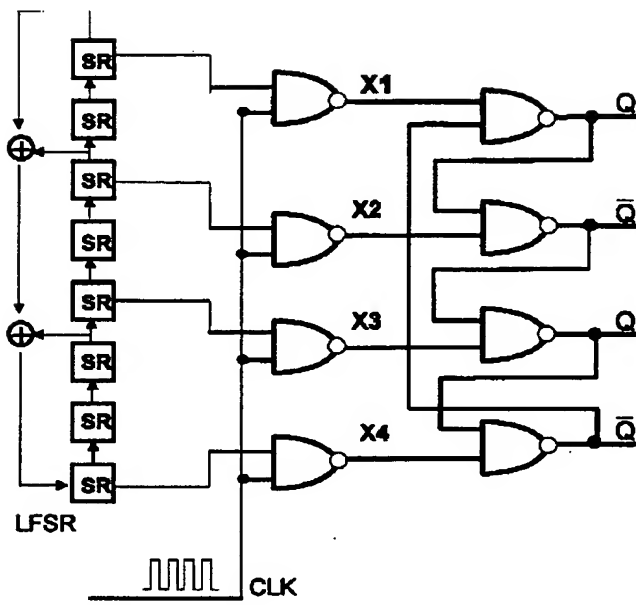
【図15】



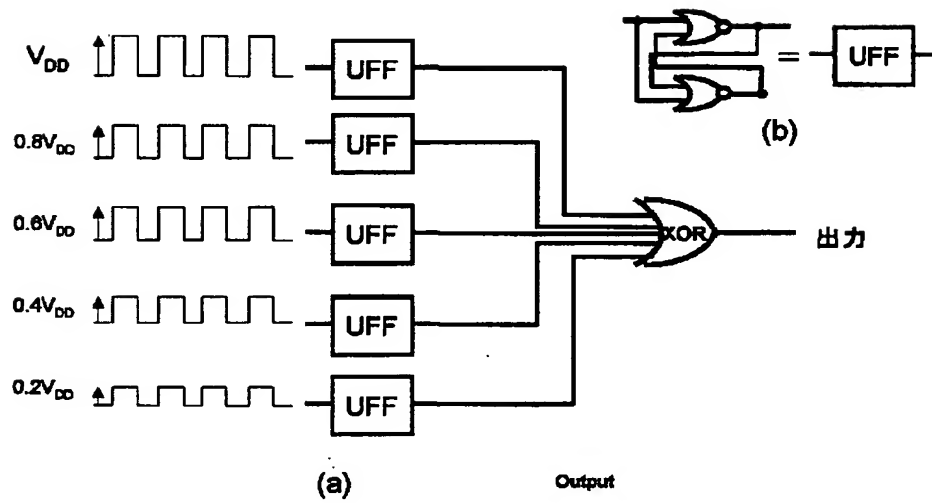
【図16】



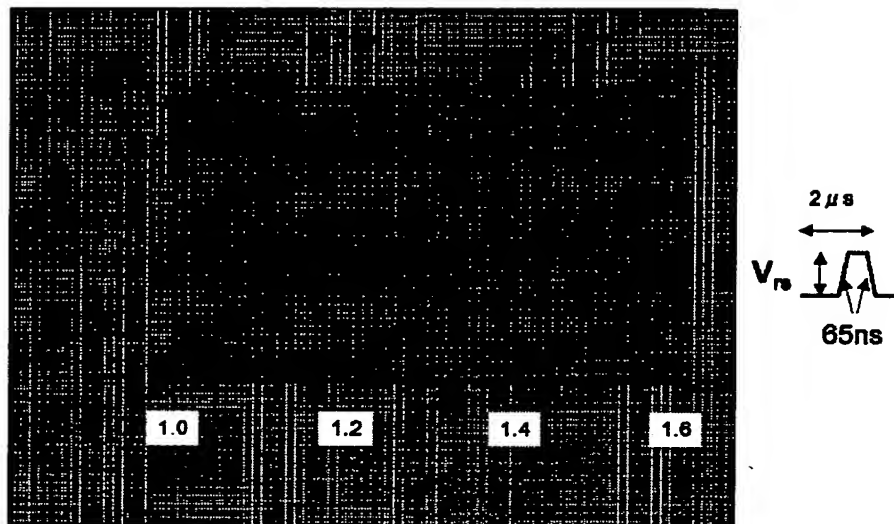
【図17】



【図18】



【図19】



フロントページの続き

(72)発明者 古賀 淳二
神奈川県横浜市磯子区新杉田町8番地 株
式会社東芝横浜事業所内

(72)発明者 大場 竜二
神奈川県横浜市磯子区新杉田町8番地 株
式会社東芝横浜事業所内
Fターム(参考) 5J049 CA03 CA10
5J104 FA01 NA04

BEST AVAILABLE COPY

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成16年10月7日(2004.10.7)

【公開番号】特開2003-173254(P2003-173254A)

【公開日】平成15年6月20日(2003.6.20)

【出願番号】特願2002-183967(P2002-183967)

【国際特許分類第7版】

G 0 6 F 7/58

G 0 9 C 1/00

H 0 3 K 3/84

【F I】

G 0 6 F 7/58 A

G 0 9 C 1/00 6 5 0 B

H 0 3 K 3/84 Z

【手続補正書】

【提出日】平成15年9月25日(2003.9.25)

【手続補正1】

【補正対象書類名】図面

【補正対象項目名】図3

【補正方法】変更

【補正の内容】

【図 3】

